UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/023,852	12/21/2001	Paul Nicholas Gartside	01.122.01	5732

7590 01/13/2006

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
BERGER, AUBREY H	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/023,852	GARTSIDE ET AL.	
	Examiner	Art Unit	
	Aubrey H. Berger	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-6,8-17,19-22,24-33,35-38 and 40-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-6,8-17,19-22,24-33,35-38 and 40-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 10/13/2005 was received and considered.

2. Claims 1, 3-6, 8-17, 19-22, 24-33, 35-38, and 40-46 are pending.

Response to Arguments

3. Applicant's response (page 12, ¶1) amends claims 4, 5, 20, 21, 36 and 37 to overcome the objections set forth in the previous Office Action and therefore those objections are withdrawn.

4. Applicant's response (page 12, ¶2) amends claims 34-46 to overcome the §112 ¶2 rejections set forth in the previous Office Action and therefore those rejections are withdrawn.

5. Applicant's arguments with respect to claims 1-46 have been considered but are moot in view of the new ground(s) of rejection. The rejections are clarified below to further explain Hypponen.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 3-6, 8-17, 19-22, 24-33, 35-38, and 40-46 are rejected under 35 U.S.C. 102(e) as being anticipated by International Publication Number WO 02/19067 to Hypponen.

Regarding claim 1, Hypponen discloses a computer program product for controlling a computer to generate mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device (page 2, lines 13-17), said computer program product comprising:

obtaining (fig. 3) master malware definition data/antivirus software and database updates contained at the Management Center virus signature data base (fig. 1, #5) obtained via a management message/anti-virus software/database update (page 7, lines 1-4), identifying a plurality of items of malware/virus signatures, each belonging to one of a plurality of classes of malware/virus signatures, threat (page 7, lines 26-30), identifying code/software, operable to identify one or more classes of malware threat against which said mobile computing device/wireless device, is to be protected (page 8, lines 13-19), and generating code operable to generate from said master malware definition data/Management Center virus signature database, said mobile computing device/wireless device, malware definition data (fig. 3), said mobile computing device/wireless device, malware definition data/virus signature database, identifying items of malware identified within said master malware definition data/Management Center virus signature database, which are within classes of malware threat against which said mobile computing device/wireless device, is to be protected, (fig. 3, "Is message applicable to destination mobile device?"); wherein said obtaining code, said

identifying code and said generating code are executed by a fixed location computing device/Management Center (fig. 1, #5), said fixed location computer/Management Center, being operable to transfer (fig. 3, "Send message via transit network") to said mobile computing device/wireless device, one or more computer files/antivirus software/database update, including at least a computer file containing said mobile computer device/wireless device, malware definition data/management message/antivirus software/database update, (fig. 3); wherein said fixed location computing device/Management Center, stores profile data identifying one or more different types of mobile computing device/wireless devices/subscribers (Fig 1, #2, #4, & page 5, line 24-26), to which said fixed location computing device/Management Center, may transfer computer files/antivirus software/database update, and corresponding threat data identifying one or more classes of malware/virus signatures, threat to which each of said mobile computing devices/wireless devices, is vulnerable (fig. 3, sequence number is compared, page 7, lines 1-5, & page 4, lines 22-25); wherein only a subset of said master malware definition is used to generate said mobile computing device malware definition data (fig. 3, "Is message applicable to destination mobile device?") for tailoring said mobile computing device malware definition data to accommodate only malware threats to which said mobile computing device is vulnerable (page 4, lines 22-25 & page 8, lines 13-19 & page 10, lines 28-32).

Regarding claim 3, Hypponen further discloses wherein said fixed location computing device/Management Center, is a user computer (Fig. 1, #7), having

communication link with said mobile computing device/wireless device, (page 6, lines 24-26).

Regarding claims 4-6, Hypponen further discloses wherein, when said mobile computing device/wireless device, is connected to said fixed location computing device/Management Center, different versions of user generated computer files respectively stored by said mobile computing device/wireless device, and said fixed location computing device/Management Center, are synchronized (fig. 3, "Is sequence number expected?"), wherein said mobile computing device/wireless device, malware definition data/virus signature database, is transferred from said fixed location computing device/Management Center, to said mobile computing device/wireless device, during said synchronization (fig. 3), when said mobile computing device/wireless device, is connected to said fixed location computing device/Management Center, versions of said mobile computing device/wireless device, malware definition data/virus signature database, stored on said mobile computing device (virus signature database) and said fixed location computing device/Management Center, are compared (fig. 3), and, if said fixed location computing device/Management Center, has a more up-to-date version of said mobile computing device/wireless device, malware definition data/virus signature database, then said more up-to-date version/database update, of said mobile computing device/wireless device, malware definition data/virus signature database/database update is transferred from said fixed location computing device/Management Center, to said mobile computing device/wireless device (page 3,

lines 5-7 & page 4, lines 22-25 & page 7, lines 10-20).

Regarding claims 8-10, Hypponen further discloses wherein user controlled policy data (fig. 2, #8-10), is used in combination with said threat data to control against which classes of malware threat said mobile computing device/wireless device, is protected by said mobile computing device/wireless device, malware definition data (page 6, lines 20-25), wherein said different types of mobile computing device/wireless devices, correspond to different types of operating system (page 5, line 16), computer program used by mobile computing devices/wireless devices, wherein said fixed location computer/Management Center, device detects to which mobile computing devices/wireless devices, it may transfer computer files by detecting installation upon said fixed location computing device/Management Center, of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices/wireless devices (page 5, line 19 to page 6, line 4).

Regarding claims 11-13, Hypponen further discloses wherein fixed location computing device/Management Center, also transfers a malware scanner computer program/anti-virus software (fig. 1, page 5, lines 5-6) from said data source to said mobile computing device/wireless device wherein said fixed location computing device/Management Center, checks for an updated malware scanner computer program becoming available from said data source and if such an updated malware

scanner computer program become available then obtains said updated malware scanner computer program/ anti-virus scanning engine, for transfer to said mobile computing device/wireless device (page 6, lines 21-24 & fig. 3).

Regarding claim 14, Hypponen further discloses wherein said master malware definition data/Management Center virus signature database is also used to protect said fixed location computing device/Management Center, from malware (Fig. 1, #11).

Regarding claim 15, Hypponen further discloses wherein said fixed location computing device/Management Center, is connected to said data source by a fixed Internet link (page 2, lines1-2).

Regarding claim 16, Hypponen further discloses wherein said items of malware include one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image (page 1, ¶4).

As per claims 17, 19-22, and 24-32, these are a method version of the claimed computer program product discussed above in claims 1, 3-6, and 8-16 respectively, wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claims 33, 35-38 and 40-46, these are a apparatus version of the claimed computer program product discussed above in claims 1, 3-6, and 8-16 respectively, wherein all claimed limitations have also been addressed and/or cited as set forth above.

Regarding claim 47, the computer program product as claimed in claim 1, wherein said fixed location device/Management Center, stores policy data including user defined settings identifying the manner in which said profile data is to be interpreted (page 5, lines 29 to page 6, line 4, & page 7, lines 1-5 & page 8, lines 10-23).

Regarding claim 48, the computer program product as claimed in claim 1, wherein said one or more classes of malware threat against which said mobile computing device/wireless device, is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device/wireless device, and classes for which it is desired to protect said mobile computing device/wireless device, according to user defined policies (page 8, lines 10-23).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. U.S. Patent Application Publication Number 2004/0010579 is cited for disclosing a method of managing a wireless device.

b. U.S. Patent Number 5,948,104 is cited for disclosing a method and system for updating virus signature files of a computer system.

c. U.S. Patent Application Publication Number 2002/0042886 is cited for disclosing a method of protecting a wireless device against viruses and maintaining a database of virus signatures.

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Berger whose telephone number is (571)272-

8155. The examiner can normally be reached on Monday - Thursday, 7:30 a.m. - 5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AHB

AHB

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100